From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Friday, September 09, 2022 12:01:41 PM ET

Paul,

As noted in my previous email, "NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices." For applications such as DNSSEC, where both public key and signature size are a concern, these schemes would likely be the ones of most interest (in addition to those already selected).
Separately from the interest in general-purpose signature schemes, NIST understands that some applications would benefit from signature sizes that are substantially smaller than those of Dilithium or Falcon even if the schemes had relatively large public key sizes. Certificate transparency happens to be one example that is well known and that is part of a widely-used protocol (HTTP over TLS). As Bas noted, CT involves a small number of public keys that are distributed out-of-band and a large number of signatures (2 or more per initial TLS handshake) that are distributed in-band. There are other applications where accepting (potentially) much larger public keys in exchange for much smaller signatures would be a good tradeoff, but CT is likely the most well known and most widely used one.
We would expect some submissions to target the non-lattice-based general-purpose use case and some to target the small-signature use case. We were not necessarily expecting to receive any submissions that would be good general-purpose signature schemes that also had small signatures and fast verification.

Dustin

From: pqc-forum@list.nist.gov on behalf of Paul Hoffman
Sent: Tuesday, September 6, 2022 5:42 PM
To: pqc-forum
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Sep 6, 2022, at 1:15 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
> For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification.

Can you say more about the motivation here? Are you forcusing on schemes that have possibly-giant

keys but short signatures, or are you still hoping for schemes that have a variety of different key/signature size balances? I ask as someone who supports a protocol (DNSSEC) that is concerned with delivering both keys and signatures, so size of each will matter to us.

--Paul Hoffman

--

From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Friday, September 09, 2022 12:06:38 PM ET
Attachments: smime.p7m

Does it mean that NIST is not interested in lattice-based schemes?

I have in mind specifically https://eprint.iacr.org/2022/1155.pdf , which IMHO would be nice to see considered for Round 4.

Thanks!

--

V/R,

Uri

There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.

The other is to make it so complex there are no obvious deficiencies.

- C. A. R. Hoare

> **From:** "'Moody, Dustin (Fed)' via pqc-forum"
> **Reply-To:** Dustin Moody
> **Date:** Friday, September 9, 2022 at 12:02
> **To:** Paul Hoffman , pqc-forum
> **Subject:** Re: [Ext] [pqc-forum] Call for Additional Signatures is released
>
> Paul,
>
> As noted in my previous email, "NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices." For applications such as DNSSEC, where both public key and signature size are a concern, these schemes would likely be the ones of most interest (in addition to those already selected).

Separately from the interest in general-purpose signature schemes, NIST understands that some applications would benefit from signature sizes that are substantially smaller than those of Dilithium or Falcon even if the schemes had relatively large public key sizes. Certificate transparency happens to be one example that is well known and that is part of a widely-used protocol (HTTP over TLS). As Bas noted, CT involves a small number of public keys that are distributed out-of-band and a large number of signatures (2 or more per initial TLS handshake) that are distributed in-band. There are other applications where accepting (potentially) much larger public keys in exchange for much smaller signatures would be a good tradeoff, but CT is likely the most well known and most widely used one.

We would expect some submissions to target the non-lattice-based general-purpose use case and some to target the small-signature use case. We were not necessarily expecting to receive any submissions that would be good general-purpose signature schemes that also had small signatures and fast verification.

Dustin

From: pqc-forum@list.nist.gov on behalf of Paul Hoffman
Sent: Tuesday, September 6, 2022 5:42 PM
To: pqc-forum
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Sep 6, 2022, at 1:15 PM, 'Moody, Dustin (Fed)' via pqc-forum wrote:
> For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification.

Can you say more about the motivation here? Are you forcusing on schemes that have possibly-giant keys but short signatures, or are you still hoping for schemes that have a variety of different key/signature size balances? I ask as someone who supports a protocol (DNSSEC) that is concerned with delivering both keys and signatures, so size of each will matter to us.

--Paul Hoffman

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-

forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/13C6E198-B827-434C-9EF8-1AA8609A8DDD%40icann.org.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86699EFD77C84C6C5902613EE5439%40SA1PR09MB8669.namprd09.prod.outlook.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/9B454A1B-4533-49A9-A0F9-74CF81F6BEF6%40ll.mit.edu.

From: Fx FRT <talaverafructifera@gmail.com> via pqc-forum@list.nist.gov
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Saturday, September 10, 2022 05:12:32 PM ET

Paul Hoffman <paul.h...@icann.org>, pqc-forum <pqc-...@list.nist.gov>
<>

[10/9 22:47] Fx FRT: Es computación post cuántica que creo es lattide por ataques a la GPS y drones de control etc y trazan rectas cuando aprenderán a tomar el punto más próximo entre ellos P, Q, son el producto y puntos iniciales de una trayectoria cualesquiera ahora ponemos rectas en pos de la trayectoria cualesquiera que imponga el recorrido para hacer la ruta más próxima solo hay que suponer que si el metro unidad tuviera un metro cualesquiera de rectificación y longitud es decir un medio al cuadrado más un medio al cuadrado todo raiz elevado cada medio al cuadrado en si mismo sería igual a uno ahora haz el conjugado mod 6 de un cubo el cubo mod 6 de un metro lok partes en partes iguales para que sea la cifra más grande la Grande solo hace falta mod 6 en linea con lo cual el sumatorio de un cubo mínimo sería partir de un cubo y hacer un hipercubo √(1/2) ²+(1/2) ²+(1/3) ²= 9,827 que es el hipercubo de un hexaedro de parte maxima de un metro hipercubo o por ahí de máxima longitud permisiva pero si lo quieres hacer del mínimo tamaño solo tienes que ramdom separó líneas entre matriz cúbica recuerda que esto son 6 lados y mod 6 es la parte que buscamos entre 1 mm 3 mm 3 mm 3 mm 9mm 3mm 3mm 3mm 24mm 3 mm 3mm 3mm 9mm 3mm 3mm 3mm 1mm 51 +51 = 102 y partes de 1 mm para dibujar la trayectoria más corta la cantidad 49 es la más corta y cualesquiera de las otras cantidades sería en mod 6, 6.16666666 asike en mod 6 16666666∞es la parte que corresponde menos 1 mm a la parte más corta que es un mm ya que mod (6) de (49,6.166666etc) entonces en mod(6) que se rompe de 1 en 0.98 en mod (5) tienes la respuesta por que 1,66666 el resto del cociente de mod (6) suma 0.99666666 y eso si le pones 51 encima en mod (5) es 0.99911 que más 0.99999 en mod (5) que sería 999999 también y aún así es más pequeño que un metro con lo cual he demostrado el teorema de mod 5 de computación estable de menos de 1mm de conjugado de garden

[10/9 22:48] Fx FRT: Goliot queda resuelto busca goliot o cuadrado mínimo de goliot 1mm mínimo

[10/9 22:48] Fx FRT: Para un metro unidad

[10/9 22:48] Fx FRT: Y que no sobrepase ese mm por que sino se pega la Ostia y te mata tio

El vie., 9 sept. 2022 18:07, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> escribió:

> Does it mean that NIST is not interested in lattice-based schemes?
>
> I have in mind specifically https://eprint.iacr.org/2022/1155.pdf , which IMHO would be nice to see considered for Round 4.
>
> Thanks!
>
> --
>
> V/R,
>
> Uri
>
> *There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.*
>
> *The other is to make it so complex there are no obvious deficiencies.*
>
> *- C. A. R. Hoare*
>
> ---
>
> **From:** "'Moody, Dustin (Fed)' via pqc-forum" <pqc-forum@list.nist.gov>
> **Reply-To:** Dustin Moody <dustin.moody@nist.gov>
> **Date:** Friday, September 9, 2022 at 12:02
> **To:** Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
> **Subject:** Re: [Ext] [pqc-forum] Call for Additional Signatures is released
>
> Paul,
>
> As noted in my previous email, "NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices." For applications such as DNSSEC, where both public key and signature size are a concern, these schemes would likely be the ones of most interest (in addition to those already selected).
>
> Separately from the interest in general-purpose signature schemes, NIST understands that some applications would benefit from signature sizes that are substantially smaller than those of Dilithium or Falcon even if the schemes had relatively large public key sizes. Certificate transparency happens to be one example that is well known and that is part of a widely-used protocol (HTTP over TLS). As Bas

noted, CT involves a small number of public keys that are distributed out-of-band and a large number of signatures (2 or more per initial TLS handshake) that are distributed in-band. There are other applications where accepting (potentially) much larger public keys in exchange for much smaller signatures would be a good tradeoff, but CT is likely the most well known and most widely used one.

We would expect some submissions to target the non-lattice-based general-purpose use case and some to target the small-signature use case. We were not necessarily expecting to receive any submissions that would be good general-purpose signature schemes that also had small signatures and fast verification.

Dustin

From:pqc-forum@list.nist.gov on behalf of Paul Hoffman
Sent: Tuesday, September 6, 2022 5:42 PM
To: pqc-forum
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Sep 6, 2022, at 1:15 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
> For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification.

Can you say more about the motivation here? Are you forcusing on schemes that have possibly-giant keys but short signatures, or are you still hoping for schemes that have a variety of different key/signature size balances? I ask as someone who supports a protocol (DNSSEC) that is concerned with delivering both keys and signatures, so size of each will matter to us.

--Paul Hoffman

--

> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86699EFD77C84C6C5902613EE5439%40SA1PR09MB8669.namprd09.prod.outlook.com.

> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/9B454A1B-4533-49A9-A0F9-74CF81F6BEF6%40ll.mit.edu.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAOP7cWaOm%3Do%3Dq34N%2B23s-APWF4j%3DHiw8r6XNyrWe%2BQsF5%2BNPJQ%40mail.gmail.com.

From: Fx FRT <talaverafructifera@gmail.com> via pqc-forum@list.nist.gov
To: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu>
CC: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released
Date: Saturday, September 10, 2022 05:22:41 PM ET

Mod 6 mod 5 49 51 = 1 congugacion erronea si mod 6 se le añade mod (5) (49 51) =1 pero da igual por qué para añadir mod (5) estricto hasta con añadir el conjugado mod(5) 49,49 lo cual =0.91 más 0.99 tenemos 1.9 que dividido entre 2 da 0.95
5 mm para que el GPS pase de constrictor a ataque pero a hawk company le vendra bien 👍

El sáb., 10 sept. 2022 23:11, Fx FRT <talaverafructifera@gmail.com> escribió:

> Paul Hoffman <paul.h...@icann.org>, pqc-forum <pqc-...@list.nist.gov>
> <>
>
> [10/9 22:47] Fx FRT: Es computación post cuántica que creo es lattide por ataques a la GPS y drones de control etc y trazan rectas cuando aprenderán a tomar el punto más próximo entre ellos P, Q, son el producto y puntos iniciales de una trayectoria cualesquiera ahora ponemos rectas en pos de la trayectoria cualesquiera que imponga el recorrido para hacer la ruta más próxima solo hay que suponer que si el metro unidad tuviera un metro cualesquiera de rectificación y longitud es decir un medio al cuadrado más un medio al cuadrado todo raiz elevado cada medio al cuadrado en si mismo sería igual a uno ahora haz el conjugado mod 6 de un cubo el cubo mod 6 de un metro lok partes en partes iguales para que sea la cifra más grande la Grande solo hace falta mod 6 en linea con lo cual el sumatorio de un cubo mínimo sería partir de un cubo y hacer un hipercubo √(1/2) ²+(1/2) ²+(1/3) ²= 9,827 que es el hipercubo de un hexaedro de parte maxima de un metro hipercubo o por ahí de máxima longitud permisiva pero si lo quieres hacer del mínimo tamaño solo tienes que ramdom separó líneas entre matriz cúbica recuerda que esto son 6 lados y mod 6 es la parte que buscamos entre 1 mm 3 mm 3 mm 3 mm 9mm 3mm 3mm 3mm 24mm 3 mm 3mm 3mm 9mm 3mm 3mm 3mm 1mm 51 +51 = 102 y partes de 1 mm para dibujar la trayectoria más corta la cantidad 49 es la más corta y cualesquiera de las otras cantidades sería en mod 6, 6.16666666 asike en mod 6 16666666∞es la parte que corresponde menos 1 mm a la parte más corta que es un mm ya que mod (6) de (49,6.166666etc) entonces en mod(6) que se rompe de 1 en 0.98 en mod (5) tienes la respuesta por que 1,66666 el resto del cociente de mod (6) suma 0.99666666 y eso si le

pones 51 encima en mod (5) es 0.99911 que más 0.99999 en mod (5) que sería 999999 también y aún así es más pequeño que un metro con lo cual he demostrado el teorema de mod 5 de computación estable de menos de 1mm de conjugado de garden

[10/9 22:48] Fx FRT: Goliot queda resuelto busca goliot o cuadrado mínimo de goliot 1mm mínimo

[10/9 22:48] Fx FRT: Para un metro unidad

[10/9 22:48] Fx FRT: Y que no sobrepase ese mm por que sino se pega la Ostia y te mata tio

El vie., 9 sept. 2022 18:07, Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> escribió:

> Does it mean that NIST is not interested in lattice-based schemes?
>
> I have in mind specifically https://eprint.iacr.org/2022/1155.pdf , which IMHO would be nice to see considered for Round 4.
>
> Thanks!
>
> --
>
> V/R,
>
> Uri
>
> *There are two ways to design a system. One is to make it so simple there are obviously no deficiencies.*
>
> *The other is to make it so complex there are no obvious deficiencies.*
>
> *- C. A. R. Hoare*
>
> ---
>
> **From:** "'Moody, Dustin (Fed)' via pqc-forum" <pqc-forum@list.nist.gov>
> **Reply-To:** Dustin Moody <dustin.moody@nist.gov>
> **Date:** Friday, September 9, 2022 at 12:02
> **To:** Paul Hoffman <paul.hoffman@icann.org>, pqc-forum <pqc-forum@list.nist.gov>
> **Subject:** Re: [Ext] [pqc-forum] Call for Additional Signatures is released
>
> Paul,

As noted in my previous email, "NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices." For applications such as DNSSEC, where both public key and signature size are a concern, these schemes would likely be the ones of most interest (in addition to those already selected).

Separately from the interest in general-purpose signature schemes, NIST understands that some applications would benefit from signature sizes that are substantially smaller than those of Dilithium or Falcon even if the schemes had relatively large public key sizes. Certificate transparency happens to be one example that is well known and that is part of a widely-used protocol (HTTP over TLS). As Bas noted, CT involves a small number of public keys that are distributed out-of-band and a large number of signatures (2 or more per initial TLS handshake) that are distributed in-band. There are other applications where accepting (potentially) much larger public keys in exchange for much smaller signatures would be a good tradeoff, but CT is likely the most well known and most widely used one.

We would expect some submissions to target the non-lattice-based general-purpose use case and some to target the small-signature use case. We were not necessarily expecting to receive any submissions that would be good general-purpose signature schemes that also had small signatures and fast verification.

Dustin

From:pqc-forum@list.nist.gov on behalf of Paul Hoffman
Sent: Tuesday, September 6, 2022 5:42 PM
To: pqc-forum
Subject: Re: [Ext] [pqc-forum] Call for Additional Signatures is released

On Sep 6, 2022, at 1:15 PM, 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov> wrote:
> For certain applications, such as certificate transparency, NIST may also be interested in signature schemes that have short signatures and fast verification.

Can you say more about the motivation here? Are you forcusing on schemes that have possibly-giant keys but short signatures, or are you still hoping for schemes that have a variety of different key/signature size balances? I ask as someone who supports a protocol (DNSSEC) that is concerned with delivering both keys and

> > signatures, so size of each will matter to us.
> >
> > --Paul Hoffman
> >
> > --
> > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/13C6E198-B827-434C-9EF8-1AA8609A8DDD%40icann.org.
> >
> > --
> > You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> > To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> > To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86699EFD77C84C6C5902613EE5439%40SA1PR09MB8669.namprd09.prod.outlook.com.
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/9B454A1B-4533-49A9-A0F9-74CF81F6BEF6%40ll.mit.edu.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/CAOP7cWZfDp8ekhajLnMspKM70YTn8rscT1bVcxyy4_KgUjE9VQ%40mail.gmail.com.